REMARKS

This Amendment is fully responsive to the non-final Office Action dated September 8, 2008, issued in connection with the above-identified application. Claims 1-13 were previously pending in the present application. With this Amendment, claims 1, 2, 4, 5 and 10-12 have been amended; and claims 3, 6-9 and 13 have been canceled without prejudice or disclaimer to the subject matter therein. Accordingly, claims 1, 2, 4, 5 and 10-12 are all the claims that remain pending in the present application. No new matter has been introduced by the amendments made to the claims. Favorable reconsideration is respectfully requested.

In the Office Action, the specification is objected to because it contains embedded hyperlinks and/or other forms of browser-executable code. The Applicants have herein amended the specification to delete the embedded hyperlinks and/or other forms of browser-executable code noted by the Examiner. Thus, Applicants respectfully request that the Examiner withdraw the objection to the specification.

In the Office Action, claim 12 has been rejected under 35 U.S.C. 101 for being directed to non-statutory subject matter. Specifically, the Examiner alleges that the claim lacks the necessary physical articles or objects that constitute a machine or manufacture within the meaning of 35 U.S.C. 101, and that the claim is directed to functional descriptive material *per se*.

However, the Examiner also indicates that functional descriptive material recorded on a computer-readable medium will be statutory in most cases. Thus, the Applicants have amended claim 12 to indicate that the program is "recorded on a computer-readable medium." Thus, Applicants respectfully request that the Examiner withdraw the rejection under 35 U.S.C. 101.

In the Office Action, claim 4 has been rejected under 35 U.S.C. 112, second paragraph, as being indefinite. Specifically, the Examiner indicates that claim 4 recites that the hash key is obtained from the hash value and claim 3 recites that the hash value is obtained from the hash key, which creates a conflict between claims 3 and 4. The Applicants have amended the claims to clarify their scope. The Applicants note that amended claim 2 recites that the key generation unit generates the first encryption key and a first hash key based on the first and second keys and a calculation unit that calculates, using the first hash key, a first hash value for transmission data.

On the other hand, amended claim 4 recites that the key generation unit concatenates the first and second keys to generate concatenated data, calculates a third hash value for the concatenated data, and generates the first encryption key and the first hash key based on the third hash value for the concatenated data. Thus, Applicants respectfully request that the Examiner withdraw the rejection under 35 U.S.C. 112.

In the Office Action, claims 1, 2, 7 and 10-13 have been rejected under 35 U.S.C. 102(b) as being anticipated by Diffie et al. (U.S. Patent No. 5,371,794).

The Applicants have canceled claims 7 and 13 thereby rendering the above rejection to those claims moot. Additionally, the Applicants have amended independent claims 1, 2, 11 and 12 to help further distinguish the present invention from the cited prior art. As amended, claim 1 recites the following features:

"[a]n encrypted communication system comprising a first device and a second device, wherein

the first device (i) encrypts a first key using a public key of the second device to generate first encrypted data, and transmits the first encrypted data to the second device, (ii) receives second encrypted data from the second device, the second encrypted data being generated by encrypting a third key of the second device using a public key of the first device at the second device, and decrypts the second encrypted data using a secret key of the first device to obtain a second key, and (iii) generates, based on the first and second keys, a first encryption key for use in communication with the second device,

the second device (i) encrypts the third key using the public key of the first device to generate the second encrypted data, and transmits the second encrypted data to the first device, (ii) receives the first encrypted data from the first device, and decrypts the first encrypted data using a secret key of the second device to obtain a fourth key, and (iii) generates, based on the third and fourth keys, a second encryption key for use in communication with the first device, and

the first and second devices perform encrypted communication using the first and second encryption keys

wherein the first device generates the first encryption key and a first hash key based on

the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device, and

wherein the second device generates the second encryption key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matched the calculated second hash value." (Emphasis added)

The features emphasized above in claim 1 are similarly recited in independent claims 2, 11 and 12. Specifically, claim 2 recites a related communication device, claim 11 recite a related method, and claim 12 recites a related computer program. Additionally, the features noted above are fully supported by the Applicants' disclosure (see e.g., page 10, line 19 - page 11, line 5 and page 12, line 17 - page 13, line 4).

The present invention (as recited in claim 1 and similarly recited in claims 2, 11 and 12) is directed to an encrypted communication system comprising a first device and a second device. The first device (i) encrypts a first key using a public key of the second device to generate first encrypted data, and transmits the first encrypted data to the second device, (ii) receives second encrypted data from the second device, the second encrypted data being generated by encrypting a third key of the second device using a public key of the first device at the second device, and decrypts the second encrypted data using a secret key of the first device to obtain a second key, and (iii) generates, based on the first and second keys, a first encryption key for use in communication with the second device.

The second device (i) encrypts the third key using the public key of the first device to generate the second encrypted data, and transmits the second encrypted data to the first device, (ii) receives the first encrypted data from the first device, and decrypts the first encrypted data using a secret key of the second device to obtain a fourth key, and (iii) generates, based on the third and

fourth keys, a second encryption key for use in communication with the first device. The first and second devices perform encrypted communication using the first and second encryption keys.

The first device generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device.

The second device generates the second encryption key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matches the calculated second hash value.

In the Office Action, the Examiner relies on Diffie for disclosing or suggesting all the features in independent claims 1, 2, 11 and 12. However, the Applicants assert that Diffie fails to disclose or suggest the feature now recited in independent claims 1, 2, 11 and 12 (as amended).

Diffie discloses a method and apparatus for providing a secure wireless communication link between a mobile device (a mobile) and a base computing unit (a base). In Diffie, the mobile sends to the base a host certificate (Cert Mobile). When the base determines that the Cert Mobile is valid, the base sends to the mobile a Cert Base, and random number (RN1) encrypted in mobile's pubic key. The base saves the RN1 value. When the mobile validates the Cert_Base, the mobile determines the RN1 value by decrypting the encrypted RN1 using the mobile's private key. The mobile generates RN2 and generates the session key from RN1 and RN2, and encrypts RN2 using the base's public key. The mobile sends to the base the encrypted RN2. The base decrypts the encrypted RN2 using the base's private key. The base determines the session key from RN1 and RN2. The mobile and the base enter a data transfer phase using

encrypted data that is decrypted using the session key, which is RN1 and RN2 (see e.g., abstract and Figs. 5a and 5b).

However, Diffie fails to disclose or suggest a system in which the first device that generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device.

Additionally, Diffie fails to disclose or suggest a second device that generates the second encryption key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matches the calculated second hash value, as recited in independent claim 1 and similarly recited in independent claims 11 and 12.

Similarly, Diffie fails to disclose or suggest a communication device that generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for transmission data, encrypts the transmission data using the first encryption key to generate encrypted transmission data, and transmits the first hash value and the encrypted transmission data to the other device, as recited in independent claim 2. Diffie also fails to disclose a communication device that receives from the other device a second hash value for second transmission data and encrypted second transmission data, the other device generates the second encryption key and a second hash key based on the third and fourth keys, calculates using the second hash key the second hash value for the second transmission data, encrypts the second transmission data using the second encryption key to generate encrypted second transmission data, and transmits the second hash value and the encrypted second transmission data to the communication device, as recited in independent claim 2.

Diffie further fails to disclose or suggest a communication device that decrypts the encrypted second transmission data using the first encryption key, calculates using the first hash

key a second hash value for the decrypted second transmission data, and determines that the second transmission data is not tampered when the received second hash value matches the calculated second hash value, as recited in independent claim 2.

Thus, independent claims 1, 2, 11 and 12 (as amended) are not believed to be anticipated or rendered obvious by Diffie. Likewise, claim 10 is not believed to be anticipated or rendered obvious by Diffie at least based on it dependency from independent claim 2.

In the Office Action, claims 3, 5 and 6 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie in view of Devadas et al. (U.S. 2003/0204743, hereafter "Devadas"). As noted above, claims 3 and 6 have been canceled rending the above rejection to those claims moot. And, claim 5 depends from independent claim 2. As noted above, Diffie fails to disclose or suggest the features noted above in independent claim 2. Moreover, after a detailed review of Devadas, the reference fails to overcome the deficiencies noted above in Diffie.

Specifically, in setting forth the rejection, the Examiner relies on Devadas for disclosing or suggesting features which the Examiner admits is lacking in the Diffie. Regarding the Devadas reference, the Applicants note that ¶ [0212] of the reference teaches that an owner 234 sends an old challenge and a new pre-challenge to a CPUF chip 48. The new pre-challenge is passed through a hash module 191 to generate a new challenge. The new challenge is passed through a PUF circuit 100 to generate a new response. On the other hand, the old challenge is passed through the PUF circuit 100 to generate an old response. The old response is passed through a hash module h2 193 to generate a secret key. The secret key is used by an encryption and MAC module 195 to encrypt the message and generate a MAC for the encrypted message. The encrypted message and the MAC is sent out of the chip and forwarded to the owner 234.

However, Devadas fails to disclose or suggest a system in which the first device that generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device. Devadas also fails to disclose or suggest a second device that generates the second encryption

key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matches the calculated second hash value.

Similarly, Devadas fails to disclose or suggest a communication device that generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for transmission data, encrypts the transmission data using the first encryption key to generate encrypted transmission data, and transmits the first hash value and the encrypted transmission data to the other device, as recited in independent claim 2.

Devadas also fails to disclose or suggest a communication device that receives from the other device a second hash value for second transmission data and encrypted second transmission data, the other device generates the second encryption key and a second hash key based on the third and fourth keys, calculates using the second hash key the second hash value for the second transmission data, encrypts the second transmission data using the second encryption key to generate encrypted second transmission data, and transmits the second hash value and the encrypted second transmission data to the communication device, as recited in independent claim 2.

Devadas further fails to disclose or suggest a communication device that decrypts the encrypted second transmission data using the first encryption key, calculates using the first hash key a second hash value for the decrypted second transmission data, and determines that the second transmission data is not tampered when the received second hash value matches the calculated second hash value, as recited in independent claim 2.

Instead, Devadas merely teaches that a hash module h2 193 generates one secret key based on the old response (see e.g., ¶ [0212] and Fig.21). In other words, in Devadas, the one secret key is generated NOT based on both the old response and the new response, and two types of keys are not generated based on the one old response. Devadas also merely teaches that the encryption and MAC module 195 encrypts the message and generates a MAC for the encrypted

message using the one secret key (see e.g., ¶ [0212] and Fig.21). In other words, in Devadas, the message is encrypted using the one secret key, and the MAC for the encrypted message is calculated using the same one secret key.

Thus, Devadas does not contain any disclosures regarding a device that generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to another device.

Additionally, Devadas fails to disclose or suggest the above features, Devadas does not contain any disclosures regarding a system which includes a device that generates the second encryption key and a second hash key based on the third and fourth keys, receives from another device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matches the calculated second hash value.

Therefore, no combination of Diffie and Devadas would result in, or otherwise render obvious, claim 5 based at least on its dependency from independent claim 2.

In the Office Action, claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie in view of Devadas and Moris et al. (US 2003/0093669, hereafter "Moris").
Claim 4 depends from claim 2. Additionally, the Applicants respectfully submit that Moris fails to overcome the deficiencies noted above in Diffie and Devadas, with respect to claim 2. Accordingly, the Applicants submit that claim 4 is patentable at least by virtue of its dependency from independent claim 2. Finally, in the Office Action, claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie in view of Matsui et al. (US 2003/0041253). As noted above, claims 8 and 9 will have been canceled thereby rending the above rejection to those claims moot.

In light of the above, the Applicants respectfully submit that all the pending claims are patentable over the prior art of record. The Applicants respectfully request that the Examiner

withdraw the rejections presented in the Office Action dated September 8, 2008, and pass the present application to issue.

Respectfully submitted,

Yuichi FUTA et al.

/Mark D. Pratt/

By: 2008.10.21 15:06:51 -04'00'

Mark D. Pratt
Registration No. 45794
Attorney for Applicants

MDP/ats
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
October 21, 2008